Standard Operating Procedure

Number:	UM/17/SOP/NHSIGTK007		
Title:	Destruction and Disposal of Sensitive Data on Isilon Procedure		
Version:	2.3	**Effective Date**	21/11/2022
Author:	Mary McDerby	**Review Date**	11/02/2024
Reviewed by : Simon Hood		**Approved By:** Nalin Thakker	
Position: Head of Research IT Infrastructure		**Position:** Associate Vice President for Compliance, Risk & Research Integrity	
Signature:		**Signature:**	

Version	**Date**	**Reason for change**
2	21/06/2019	Review (update contents box with page numbers and remove item 10) (link RBE website) (added new 4.8 on reporting to NHS Digital) (update 6.1.1 on dissemination) (update 7.1.1 on name of IG master File) (update bibliography) (remove declaration sheet)
2.1	23/08/2021	Review with regards to business Isilon (Data Safe Haven storage)
2.2	11/02/2022	General review – SOPs, footnote labelling etc
2.3	17/11/2022	Section 9: SOP list update Addition of link to UoM document repository

This is a controlled document. Any printed or locally downloaded version may not be current. It is the responsibility of colleagues to ensure that the current version is accessed and followed. The current version is available at: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=52789

1 Background

All research studies using data obtained from NHS Digital must demonstrate that, should NHS Digital issue a data destruction notice, then it should be done so as required by the compliance obligations to the NHS Digital Information Governance Toolkit and the University of Manchester's overarching Data Sharing Framework Contract.

2 Purpose

This Standard Operating Procedure (SOP) describes the process by which IT Services will ensure that data is removed and destroyed from the Isilon storage and hardware, upon which the data has been used, should NHS Digital issue a data destruction notice.

This document only applies to the destruction of data on the University of Manchester business and research data storage infrastructure which is currently the EMC Enterprise solution known as Isilon. Due to the size of the two clusters currently in service (1800+ drives), architecture of the enterprise solution and NAS protocols it is not possible to physically erase the disks to HMG Infosec S5 Enhanced standard, as this would need to be done for all 1800 drives. To that end we describe an alternative method to support NHS Digital's requirements which ensures the data is disposed once a destruction notice has been issued.

3 Roles and Responsibilities

The PI and/or IG Lead are accountable to Research Compliance Committee (RCC) and responsible for ensuring that this document is observed in respect of data obtained from NHS Digital, for which they have responsibility and is stored under the authority of the University of Manchester Data Sharing Framework Contract (DSFC) and individual project Data Sharing Agreements (DSA). This includes, making all staff that access and use the data aware of this document. The PI and/or IG Lead are responsible for directing others in relation to these contracts. The University expects all persons operating on University sites to comply with the policies and any subsequent amendments and to seek to comply with all Codes of Practice issued by NHS Digital and relevant University wide and/or local Standard Operating Procedures (SOPs).

All staff accessing and using data that has been obtained from NHS Digital, under a Data Sharing Agreement, are accountable to the relevant PI and/or IG Lead for undertaking work in compliance with that DSA. All personnel accessing NHS Digital data should be fully trained on the University's IG policies and procedures.

Staff awareness of this Procedure will be audited periodically by the RGEIT. The RGEIT will submit on a quarterly basis a report to RCC that will include non-conformances and lessons learned to improve the Procedure.

4 Procedure

4.1 It is the responsibility of the PI to delete the data obtained from NHS Digital from the primary location on Isilon as detailed in a Data Sharing Agreement and System Level Security Policy should such a request be made by NHS Digital.

4.2 It is also the responsibility of the PI to remove such data from any local devices following the guidance from NHS Digital – Destruction and Disposal of Sensitive Data (see bibliography).

4.3 It is the responsibility of Research IT to ensure that permission to the primary location on Isilon is locked down after data deletion and nobody can access the data to pull it back from the snapshots.

4.4 After 35 days all snapshots (backups) will have been erased from the Research Data Storage Service (Research Isilon storage), and after 28 days from the Data Safe Haven Service (Business Isilon storage).

4.5 With regards to hardware destruction (please see Appendix A – Isilon storage has a retention policy attached), should the Isilon hardware fail it will be removed from service and shredded on site.

4.6 The hardware will be shredded and the destruction will be witnessed by a University of Manchester member of staff in the Data Centre.

4.7 The serial numbers of the disks will be retained in a log, with certification of the destruction by University of Manchester Data Centre staff.

4.8 The NHS Digital Data Destruction form should include a description of the data provided by NHS Digital (including years), information on all the touch points of the NHS Digital data, methods used to destroy the data and any evidence to support the destruction of the data on those touch points i.e., screenshots, Blancco certificates plus any other evidence. So in summary you should list where the data is downloaded to, where it is moved to etc (each storage point basically). Then in your IG Masterfile please record the following as evidence:

- Screenshots, Blancco certificates (if applicable) plus any other evidence
- NHS Digital destruction certificate
- Any communications from NHS Digital should also be stored in the IG Masterfile – this should include a confirmation of acceptance of the data destruction by NHS Digital, which should be requested if not received as it will be required if audited.

The NHS Digital Destruction certificate will need to be signed off by the Research IT Infrastructure Analyst who has supported you in destroying the data.

4.9 Compliance with this SOP is mandatory and non-compliance must be reported to the Head of Research Governance, Ethics and Integrity, who will determine the action to be undertaken. Staff must note that any breach of this Procedure may be treated as misconduct under the University's relevant disciplinary procedures and could lead to disciplinary action.

5 Consultation, Approval and Ratification Processes

5.1 Consultation and Communication with Stakeholders

All University NHS Digital data documents are written by a member of staff with relevant expertise and experience. Additional advice is sought from members of Research IT and the Information Governance Office within the University or external advisors, as necessary.

5.2 Document Approval Process

5.2.1 Standard Operating Procedures are approved by the Head of RGEIT and/or Associate Vice President for Compliance, Risk and Research Integrity.

5.5.2 Policies are ratified by the Research Compliance Committee.

6 Dissemination and Implementation

6.1 Dissemination

6.1.1 When approved, this document will be posted on the RGEIT IG Master File SharePoint site and the Data Safe Haven & NHS Digital data pages of the University's Directorate of Research and Business Engagement website. Only the current version will be available.

6.1.2 All PIs/IG Leads will be notified by email when the latest version of the document is available.

6.2 Implementation of Procedural Documents

6.2.1 Training covering the contents of this document is delivered by RIT and RGEIT.

6.2.2 Support and advice on the implementation of this document can be obtained via the Research Governance Officer (RGO) with responsibilities for NHS Digital data within the RGEIT.

7 Review, Monitoring Compliance with and the Effectiveness of Procedural Documents

7.1 Process for Monitoring Compliance and Effectiveness

7.1.1 The RGO will monitor compliance through regular audits of IG master files.

7.1.2 Document contents will be reviewed against any changes to the applicable guidelines and regulations and taking into account any feedback received from Researchers or IG Leads, as well as changes in Research IT infrastructure.

7.1.3 The outcome of the review - and any resulting amendments – will be reported to the Research Compliance Committee.

7.2 Standards and Key Performance Indicators 'KPIs'

7.2.1 This document will be available on the University intranet.

7.2.2 This document must be reviewed at least every two years or when there are significant changes.

7.2.3 Awareness of the document will be delivered at University IG NHS Digital training sessions delivered by the RGEIT.

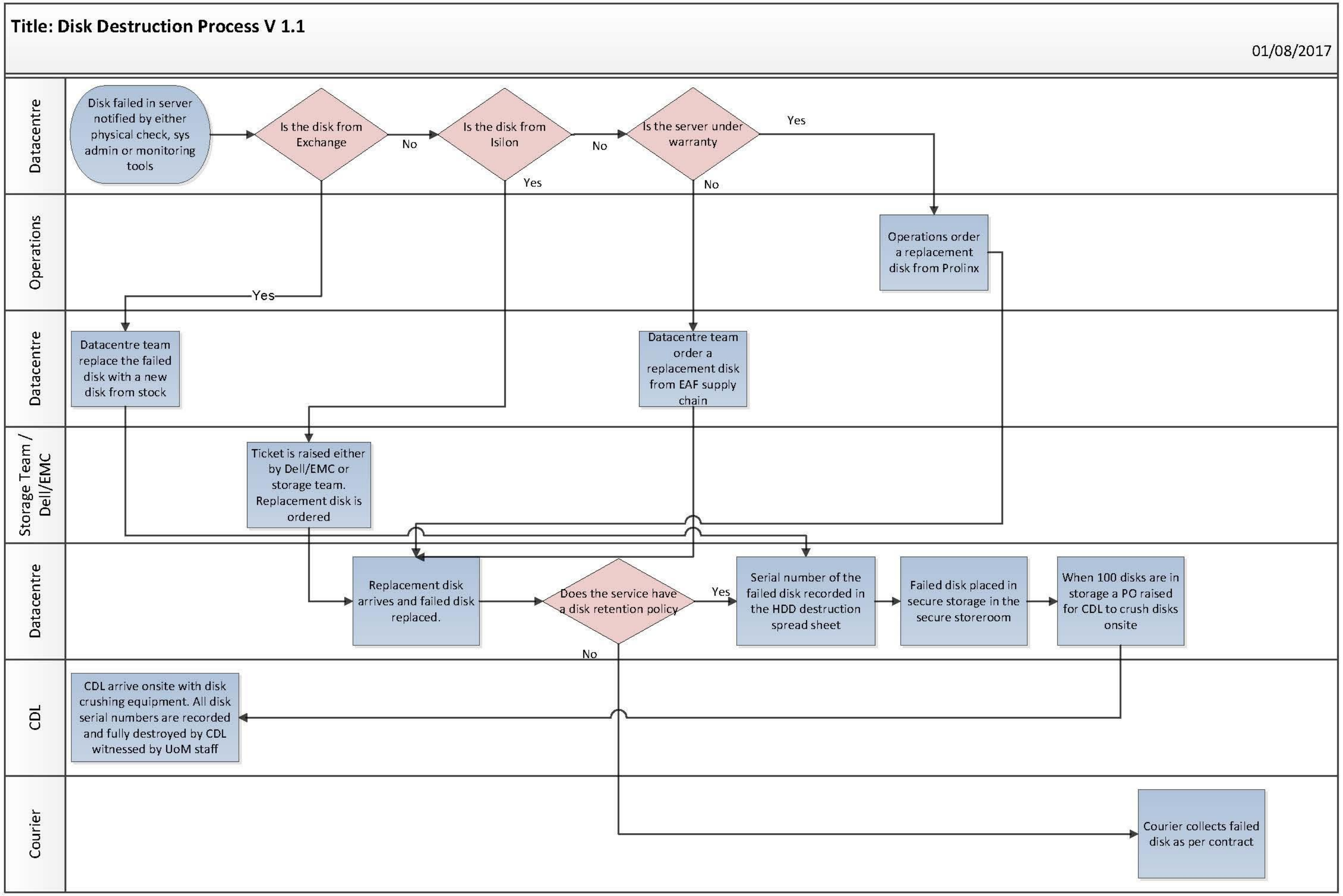
8 References and Bibliography

For NHS Digital data, the NHS Digital website, http://content.digital.nhs.uk/article/6888/DARS-Process discusses the deletion of data.

9 Associated University Documents

UM/17/SOP/NHSIGTK001:-	Risk Assessment
UM/17/SOP/NHSIGTK002:-	Confidentiality Audit Procedure
UM/17/SOP/NHSIGTK003:-	Training Needs Analysis
UM/17/SOP/NHSIGTK004:-	The Data Safe Haven

10 Appendix A:


Title: Disk Destruction Process V 1.1
01/08/2017
Datacentre
Operations
Datacentre
Storage Team / Dell/EMC
Datacentre
CDL
Courier
Disk failed in server notified by either physical check, sys admin or monitoring tools
Is the disk from Exchange
No
Is the disk from Isilon
No
Is the server under warranty
Yes
Yes
No
Operations order a replacement disk from Prolinx
Yes
Datacentre team replace the failed disk with a new disk from stock
Datacentre team order a replacement disk from EAF supply chain
Ticket is raised either by Dell/EMC or storage team. Replacement disk is ordered
Replacement disk arrives and failed disk replaced.
Does the service have a disk retention policy
Yes
No
Serial number of the failed disk recorded in the HDD destruction spread sheet
Failed disk placed in secure storage in the secure storeroom
When 100 disks are in storage a PO raised for CDL to crush disks onsite
CDL arrive onsite with disk crushing equipment. All disk serial numbers are recorded and fully destroyed by CDL witnessed by UoM staff
Courier collects failed disk as per contract